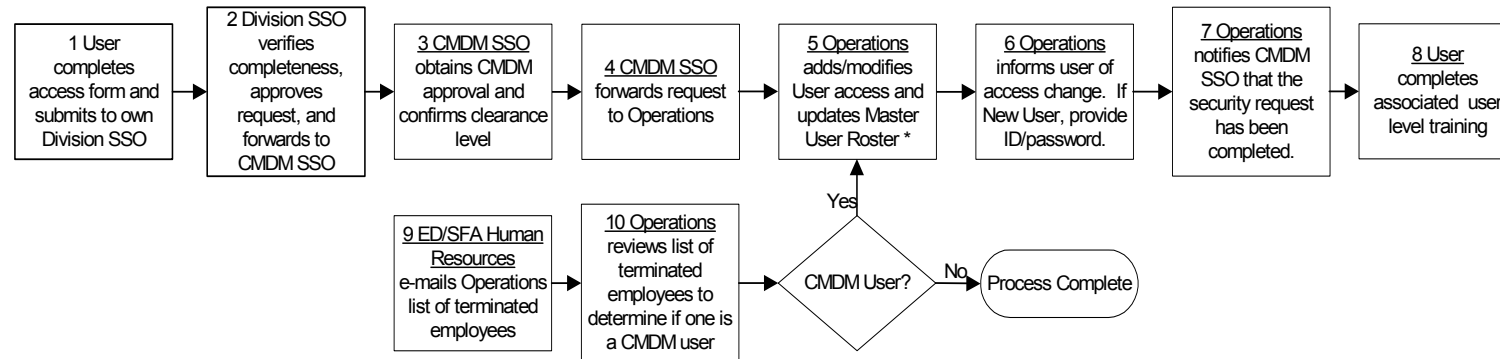## Security Access Process

Overview

This procedure provides the steps required for the future and existing Credit Management Data Mart (CMDM) Users to obtain or modify user access to the data mart.

Schematic/Detailed Process Flow

Adding a New CMDM User, Changing Security Level of an Existing User, or Terminating an Existing User

* If Terminating an Existing User, User ID will be suspended (not deleted from CMDM for audit purposes).

Responsibility

Job Title	Organization	Tasks
User	Various	▪ Completes access form and submits to own Division SSO ▪ Completes associated user level training
Division System Security Officer	Various	▪ Verifies completeness, approves request, and forwards to CMDM SSO
CMDM System Security Officer	FSA Students	▪ Obtains CMDM approval and confirms clearance level ▪ Forwards request to Operations
CMDM Operations	FSA	▪ Adds/Modifies User access and updates Master User Roster ▪ Informs user of access change. If New User, provide ID/password. (If Terminating an Existing User, User ID will be suspended (not deleted from CMDM for audit purposes)). ▪ Notifies CMDM SSO that the security request has been completed. ▪ Reviews list of terminated employees to determine if one is a CMDM user
ED/FSA Human Resources	ED/FSA	▪ E-mails Operations list of terminated employees

Procedure Trigger

Adding a New CMDM User, Changing Security Level of an Existing User, or Terminating an Existing User

Process

Adding a New CMDM User, Changing Security Level of an Existing User

1. User completes access form and submits to own Division SSO.

2. Division SSO verifies completeness, approves request, and forwards to CMDM SSO.

3. CMDM SSO obtains CMDM approval from the CMDM System Owner. In addition the CMDM SSO and confirms requestors clearance level.   The End Users require a 1C Clearance.

4. CMDM SSO forwards request to Operations to make modifications to CMDM security.

5. Operations adds/modifies User access and updates the Master User Roster. If an existing CMDM User is terminated, the User ID will be suspended. Suspended User Ids older than a determined time period will be deleted from the data mart.

6. Operations informs user of access change via a memorandum or telephone. If New User ID was created, operations will provide user with ID and password.

7. Operations notifies CMDM SSO that the security request has been completed.

8. User completes required training for security level:

CMDM User Groups	Associated Training
Web Users	Basic Web Training
Extended Web Users	Basic Web Training
	Extended Web Training
Power User	Basic Web Training
	Extended Web Training
	MicroStrategy Report Developer
	Transition Session material

Process Ends.

Terminating an Existing User
Operations can also get notification of security changes via ED/FSA Human Resources employee termination notifications.

9. ED/FSA Human Resources e-mails Operations list of terminated employees.

10. Operations reviews list of terminated employees to determine if one is a CMDM user. If a CMDM User is on termination list, proceed to Step 5: Operations suspends user access.